UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: TANEISHA ROBERTSON, *individually and on behalf of her minor children, X.R. and J.R., and all others similarly situated,* Plaintiff, v. PROGRESS SOFTWARE CORPORATION; DELTA DENTAL OF CALIFORNIA; DELTA DENTAL INSURANCE COMPANY; DELTA DENTAL PLANS ASSOCIATION, Defendants.	MDL No. 1:23-md-03083-ADB-PGL DIRECT FILED COMPLAINT & JURY DEMAND PURSUANT TO ORDER REGARDING DIRECT FILING CIVIL ACTION NO. 1:24-cv-10668-ADB

FIRST AMENDED COMPLAINT

Plaintiff Taneisha Robertson, individually and on behalf of her minor children, X.R. and J.R. and all similarly situated persons, alleges the following against Delta Dental of California ("DDCA"), Delta Dental Insurance Company ("DDIC") (together, "Delta Dental" or "Delta Dental Defendants"), Delta Dental Plans Association ("DDPA"), and Progress Software Corporation ("Progress") (collectively referred to herein as "Defendants") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

NATURE OF ACTION

1. This Complaint is being directly filed into this MDL proceeding pursuant to the Court's MDL Order No. 12.

2. Plaintiff incorporates the allegations contained in the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

3. Accordingly, Plaintiff and Class Members bring this action against Defendants, seeking redress for their unlawful conduct and asserting claims for (i) negligence, (ii) negligence per se, (iii) breach of implied contract, (iv) breach of implied covenant of good faith and fair dealing, (v) breach of confidence, (vi) unjust enrichment, (vii) invasion of privacy (public disclosure of private facts), (viii) bailment, (ix) breach of third-party beneficiary contract, (x) breach of fiduciary duty, (xi) declaratory judgment, as well as for violating the (xii) California Unfair Competition Law, (xiii) Georgia Uniform Deceptive Trade Practices Act, and (xiv) Massachusetts General Laws.

4. Plaintiff and Class Members seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including but not limited to improvements to Defendants' data security systems, future audits and penetration testers, as well as long-term and adequate credit monitoring services funded by Defendants.

PARTIES

5. Plaintiff Taneisha Robertson and her children are, and at all times mentioned herein were, individual citizens of the State of Georgia.

6. Defendant Progress Software Corporation ("Progress") is a corporation organized under the laws of the State of Delaware with its principal place of business located at 15 Wayside Road, Suite 4, Burlington, Massachusetts 01803. Progress offers file transfer solutions through its

MOVEit Transfer software, which experienced the Data Breach underlying Plaintiff's and Class Members' claims.

7. Defendant Delta Dental of California ("DDCA") is a nonprofit 501(c)(4) corporation, incorporated in California, that operates as a dental insurance provider in California. Delta Dental of California is a citizen of California with its principal place of business located at 560 Mission Street, #1300, San Francisco, California, 94105. The Delta Dental of California enterprise includes various affiliates, including Delta Dental Insurance Company, Delta Dental of the Delta Dental of Pennsylvania, Delta Dental of New York, inc., and their affiliated companies, as well as the national DeltaCare USA network. Collectively, these affiliates are referred to as "Delta Dental of California and Affiliates."

8. Delta Dental Insurance Company ("DDIC"), an affiliate of "Delta Dental of California and Affiliates," operates and administers insurance plans in Alabama, Florida, Georgia, Louisiana, Mississippi, Montana, Nevada, Utah, and Texas. It is headquartered in California at 560 Mission Street, #1300, San Francisco, CA, 94105.

9. Defendant Delta Dental Plans Association ("DDPA") is an Illinois not-for-profit national network of Delta Dental Companies, headquartered at 1515 W 22nd St # 450, Oak Brook, Illinois 60523.

JURISDICTION

10. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more Class Members are citizens of states different from Defendants.

11. Plaintiff, on her own behalf and on behalf of her children, is filing this Amended Complaint in the District of Massachusetts pursuant to the Court's MDL Order No. 12 (Direct Filing Order).

FACTUAL ALLEGATIONS

Defendants' Businesses Require the Collection and Maintenance of Plaintiff's and Class Members' Private Information

12. Plaintiff and Class Members reallege and incorporate by reference all paragraphs, from Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908).

13. "Delta Dental of California and Affiliates" is comprised of various companies,[1] and touts itself as the "nation's largest, most experienced dental benefits carrier," that offers individual and group dental insurance plans, providing dental insurance to tens of million individuals.[2] "Collectively, [Delta Dental of California and Affiliates] offer benefits to more Americans than any other dental insurance company."[3]

14. Delta Dental Insurance Company ("DDIC") is an affiliate of Delta Dental of California and Affiliates. DDIC offers and administers Delta Dental PPO and other fee-for-service dental programs to groups headquartered or located in Alabama, Florida, Georgia, Louisiana, Mississippi, Montana, Nevada and Utah, and vision programs to groups headquartered in West Virginia. In Texas, Delta Dental Insurance Company offers and administers fee-for-service dental programs and provides a dental provider organization (DPO) plan.

---

[1] "The Delta Dental of California enterprise includes its affiliates Delta Dental Insurance Company; Delta Dental of the District of Columbia, Delta Dental of Delaware, Inc., Delta Dental of Pennsylvania, Delta Dental of New York, Inc., Delta Dental of West Virginia, and their affiliated companies, as well as the national DeltaCare USA network." *Infra*, n. 16.
[2] https://perma.cc/W434-ZPCK (last visited June 4, 2024).
[3] https://perma.cc/63Q4-38XM (last visited June 4, 2024).

15. "The companies in [Delta Dental's] enterprise are members, or affiliates of members, of the Delta Dental Plans Association, a network of 39 Delta Dental companies that together provide dental coverage to 80 million people around the country."[4] Delta Dental Plans Association ("DDPA") was created in order to coordinate dental insurance for companies with employees in multiple states, and allows customers to see a provider in any state regardless of the member company through which they receive dental insurance.

16. DDPA's website, © Copyright 2024 Delta Dental Plans Association, represents the network of 39 Delta Dental Companies and is branded as "Delta Dental."

17. The other related website, © Copyright 2024 Delta Dental, "is the home of" the Delta Dental Defendants, collectively. This website also brands itself as "Delta Dental". Each of these Defendants is a member of DDPA's network of 39 Delta Dental insurance companies.

18. As described on both DDPA's website and the website for "Delta Dental of California and Affiliates, "Through our national network of Delta Dental companies, we offer dental coverage across all 50 states, Puerto Rico and other U.S. territories . . . offering dental insurance across all 50 states, D.C., and Puerto Rico."[5]

19. Upon information and belief, DDPA, the national network of Delta Dental Companies, oversees the operations of Delta Dental Companies, including Delta Dental Defendants.

20. DDPA holds itself out as having interconnected business operations with Delta Dental Defendants.

[4] Delta Dental, *2019 Social Impact Report*, available https://perma.cc/TNZ2-CMAX (last accessed June 4, 2024).
[5] Delta Dental, *About Delta Dental*, https://perma.cc/4R33-GGCQ (last accessed June 4, 2024).

21. DDPA refers to itself as one and the same as Delta Dental Defendants with respect to its value of data security and prioritizing practices to protect customers' data, *i.e.*, that its security policies and practices are consistent through its network of Delta Dental Companies, including Delta Dental Defendants.

22. Specifically, "Because security is important to both Delta Dental and you, we employ reasonable safeguards designed to promote the security of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure. Personal information is protected using various physical, administrative and/or technical safeguards in transit and at rest."[6]

23. Upon information and belief, all the Delta Dental Companies within DDPA's network, including Delta Dental Defendants, utilize the MOVEit software and follow the same safety and security policies, practices, and procedures.

24. Customers, *i.e.*, policy holders through a Delta Dental Company, can sign up for an Account with Delta Dental Plans Association, for example, to access a Member Dashboard. To complete account registration, DDPA requires the following information: first name, last name, Member ID and health insurance information, Social Security number, date of birth, ZIP code, and email address.

25. Through their DDPA accounts, members may "request information about [their] coverage or claims through the Services (which request will go to the Delta Dental Company that administers or underwrites [their] dental benefits coverage)," and DDPA requires that they provide certain sensitive personal and medical related information as part of the request. [7] Additionally,

[6] "Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers," available here: https://perma.cc/A2HD-6PW3 (last accessed June 4, 2024).
[7] *Id.*

members use DDPA's platform to track their dental activity, *i.e.*, protected health information as defined under HIPAA.[8]

26. Customers can use DDPA's landing page to locate more information about their Delta Dental insurance provider and download the Delta Dental mobile application, through which their Private Information flows. In other words, customers, including Plaintiff and Class Members, interact directly with DDPA and provide their Private Information to DDPA, in addition to the Delta Dental Company, including Delta Dental Defendants, that provides their insurance plan.

27. Branding on DDPA's website and the "Delta Dental of California and Affiliates" (comprised of Delta Dental Defendants) website is identical.

28. Additionally, DDPA's diversity, equity, and inclusion "guiding principles" apply to all Delta Dental Defendants, according to DDPA's website.

29. As part of their business operations, Delta Dental Defendants acquire, collect, store, and utilize consumers' sensitive personal data, including personal identifying information ("PII")[9] and protected health information ("PHI")[10] (collectively, "Private Information"). As a condition

---

[8] *Infra*, n. 10.

[9] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[10] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq*., and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103 *Protected health information.* "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. "Summary of the HIPAA Privacy Rule," DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/9U8X-5L7E html (last accessed June 4, 2024).

of receiving dental insurance through Delta Dental Defendants or any of the Delta Dental Companies within DDPA's national network, Plaintiff and Class Members were required to provide and entrust their highly sensitive Private Information with Delta Dental Defendants. Delta Dental Defendants relied on and derived monetary benefits and profit from Plaintiff's and Class Members' providing their Private Information.

30. DDPA also collects, transmits, and uses this data as part of its business operations, and informs users in its Privacy Policy that it "shar[es] collected personal information with third parties, including service providers, business associates, and the Delta Dental Companies."[11]

31. DDPA entered into a "Business Associate Agreement" ("BAA") with each of the Delta Dental Companies, which identifies that both entities are regulated under the U.S. Health Insurance Portability and Accountability Act (HIPAA), wherein both parties must agree that they "understand the privacy and security safeguards established by HIPAA, HITECH, and the Omnibus Rule and agree to protect member Personal Health Information (PHI)"[12] and set out the terms in which Plaintiff's and Class Members' Private Information can be transferred and disclosed. In other words, Delta Dental Defendants and DDPA share data. Similarly, DDPA derives financial benefit from Plaintiff's and Class Members' providing their Private Information to its Delta Dental Companies with which it contracts.

32. Defendant Progress represents itself as "a global supplier of products and services for business applications" that "develops, markets and distributes application development, deployment, integration and management software to business, industry and governments worldwide."[13]

---

[11] *Supra*, n. 6.
[12] *Id.*; *see also* https://perma.cc/8TUV-ED9Y (last accessed June 4, 2024).
[13] Progress, SEC Form 10-K (2003), https://perma.cc/4UMV-5C2R (last accessed June 4, 2024).

33. As alleged and incorporated herein, Progress knew its software, MOVEit, was being used to transfer sensitive information.

34. As part of its business operation with respect to its healthcare clients, Progress acquires, collects, stores, and utilizes consumers' sensitive personal data, including Private Information of its clients' customers, such as Plaintiff and Class Members.

35. Delta Dental Defendants contract with the third-party service provider, Progress, to utilize its MOVEit software to store and transfer the Private Information of Plaintiff and Class Members.

36. Similar to DDPA, Progress also entered into Business Associate Agreements, which set out the terms in which Plaintiff's and Class Members' Private Information can be transferred and disclosed.[14]

37. As business associates of healthcare providers, both DDPA and Progress knowingly obtain sensitive patient Private Information and have a resulting duty to securely maintain such information in confidence.

38. This Private Information was compromised as a result of a security vulnerability in the MOVEit software, as alleged in Plaintiffs' Omnibus Set of Additional Pleading Facts and incorporated and realleged herein. *See* ECF No. 908 (section I(D)).

39. The MOVEit Transfer servers that were targeted in the Data Breach were located within the Delta Dental of California network environment. Ex. A. Affidavit of S. Achenbaugh (DDPA), ¶ 9. As discussed, *infra*, these servers contained the Private Information of Delta Dental Defendants' customers, including Plaintiff and Delta Dental Nationwide Class Members.

[14] *See* https://perma.cc/PAG9-PYHZ (last visited June 4, 2024).

40. Although thousands of companies were affected by the Data Breach, Delta Dental "stands out [because it] is the third largest healthcare MOVEit-related breach to have been reported" – affecting 6,928,932 customers.[15]

41. The Private Information compromised in the Data Breach included "names with some combination of the following: addresses, Social Security numbers, driver's license numbers or other state identification numbers, passport numbers, financial account information, tax identification numbers, individual health insurance policy numbers, and/or health information."[16]

42. Some or all of the healthcare and/or medical information that was compromised and stolen by the unauthorized actors constitutes "protected health information" within the meaning of HIPAA.[17]

Defendants Misrepresent Their Security Practices

43. Delta Dental Defendants and DDPA made numerous representations and promises that customers' Private Health Information is "private and confidential[,]" and about its commitment to maintaining its safety, including on its various webpages.[18]

44. For example, DDPA's "Compliance Center" discusses "Delta Dental's compliance" with the various mandates under HIPAA.[19] Under its Privacy Policy, DDPA states that it "collects, uses, and discloses your individually identifiable health information consistent

[15] "Delta Dental of California Data Breach: 7 Million Individuals Affected." THE HIPAA JOURNAL, published Dec. 17, 2023, available here: https://perma.cc/WZE9-R483 (last accessed June 4, 2024).
[16] Data Breach Notifications, Office of the Maine Attorney General, "AG Notice – ME – Delta Dental + Affiliates," PDF available for download: https://perma.cc/VV48-LETD (last visited June 4, 2024).
[17] *Supra*, n. 10.
[18] *Supra*, n. 3.
[19] *See* https://perma.cc/Q3JG-ZK6Z (last visited June 4, 2024); *see also supra*, n. 3.

with the terms of applicable HIPAA business associate agreements with the Delta Dental Companies."[20]

45. DDPA also states in one of its privacy statements that, "Because security is important to both Delta Dental and you, we employ reasonable safeguards designed to promote the security of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure. Personal information is protected using various physical, administrative and/or technical safeguards in transit and at rest."[21]

46. Delta Dental Defendants' website assures existing and prospective customers that it "has updated and implemented system changes to accommodate the applicable 5010 standards and the associated transaction sets" and that HIPAA covered transactions include enrollment information in health plans and health care claims, which include costs of treatments – precisely the type of data that was compromised in the Data Breach.[22]

47. Similarly, Defendant Progress claims to be HIPAA compliant, and that it has, among other protocols, "implemented technical and organizational measures to ensure HIPAA compliance and operates in secure computing environments in its corporate offices, development environments, and production cloud products. Progress audits its security solutions and processes annually to maintain SOC2 and HIPAA validation."[23]

Defendants Owed Legal Obligations to Plaintiff and Class Members

48. DDPA's national network of 39 Delta Dental Companies (including Delta Dental Defendants) provides dental insurance to 80 million individuals. Plaintiff and Class Members are currently or were formerly customers of Delta Dental Defendants.

---

[20] *Supra*, n. 6.
[21] *Id*.
[22] https://perma.cc/U37F-DBBK (last visited June 4, 2024).
[23] https://perma.cc/G6HN-ZWJ9 (last visited June 4, 2024).

49. As a condition of using Delta Dental Defendants' services, *i.e.*, entering into a direct business relationship with a Delta Dental member company, Plaintiff and Class Members were required to provide their highly sensitive Private Information.

50. Because Delta Dental Defendants required Plaintiff's and Class Members' Private Information in exchange for the provision of dental insurance, by accepting their Private Information, Delta Dental Defendants owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information and keeping it confidential, safe, and secure from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach, including by ensuring that their third-party service providers implemented adequate, secure, and compliant safeguards to protect their own platforms.

51. Because of the highly sensitive and personal nature of the information that Delta Dental Defendants acquire, maintain on their shared network, and input into Progress's MOVEit file transfer server and/or software, Delta Dental Defendants have a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their Private Information, including to ensure their third-party vendors have implemented adequately safe and secure policies and practices.

52. Delta Dental Defendants promise, among other things, to: keep customers' files private; comply with regulation and industry standards related to data security and maintenance of its customers' files and the Private Information contained therein; only use and release Private Information for reasons that relate to the products and services Plaintiff and Class Members obtain from Defendants; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

53. Similarly, DDPA owed duties analogous to Delta Dental Defendants by representing itself to customers as one and the same, such that a reasonable person would rely on these representations in understanding the nature of their relationship. DDPA also benefitted monetarily from its collection, storage, receipt, transfer, and use of Plaintiff's and Class Members' Private Information as laid out in its BAAs.

54. Similarly, due to Defendant Progress's role as a third-party beneficiary of the business relationships between Delta Dental Defendants and Plaintiff and Class Members, and its own contractual relationship with Delta Dental Defendants for use of its MOVEit file transfer software, Defendant Progress's business relied on and benefitted from Plaintiff's and Class Members' entrusting their Private Information to Delta Dental Defendants and thus owed Plaintiff and Class Members the same duties to protect their Private Information.

55. As alleged and incorporated, Progress owed a non-delegable duty to Plaintiff and Class Members to identify and remediate vulnerabilities in its MOVEit software and to implement reasonable and adequate security measures to secure and protect Plaintiff's and Class Members' Private Information.[24]

56. As incorporated and realleged herein, Delta Dental Defendants and DDPA knew of these requirements and of industry cybersecurity standards and their obligations to protect Plaintiff's and Class Members' highly-sensitive Private Information. *See* ECF No. 908 (section V).

57. In addition to the aforementioned and incorporated industry standards, the Center for Internet Security (CIS) has also published clear guidance on the steps businesses that share

[24] *See* ECF No. 908 (section IV(C)) (describing Progress's legal and equitable duties of which it knew or should have known); these obligations also arise because it is regulated under the terms of a "Business Associate" under HIPAA. 45 C.F.R. § 160.103(1); *infra*, n. 28.

information with third parties, *e.g.*, "rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions," should take to ensure those vendors have appropriate cybersecurity systems and protocols in place, and that their customers' Private Information is adequately safeguarded. Since its formation in 2000, CIS has established applicable industry standards to help people, businesses, and governments protect themselves against pervasive cyber threats that are "globally recognized best practices for security IT systems and data."[25]

58. As incorporated and realleged herein, Progress knew of its obligations to protect Plaintiff and Class Members Private Information, including of industry cybersecurity standards, and could have prevented the Data Breach by following industry standards for secure software development and maintenance. *See* ECF No. 908 (sections III-IV).

59. Moreover, Delta Dental Defendants owed legal obligations to Plaintiff and Class Members as "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA") and subject to its regulation.[26]

60. Due to the nature of the business relationship between Progress and Delta Dental Defendants, *i.e.*, contracting for use of Progress's MOVEit software to store and transfer the "protected health information"[27] of Plaintiff and Class Members, Defendant Progress is regulated by HIPAA as a "business associate."[28]

---

[25] Center for Internet Security, *Critical Security Controls*, at 12, 42-44 (May 2021), https://perma.cc/R3M4-4KAU (last visited June 4, 2024).

[26] A "covered entity" is defined as, *inter alia*, "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by [HIPAA]." 45 C.F.R. § 160.102(a)(3). "Health Plans, including health insurance companies" are covered entities under HIPAA. *Your Rights Under HIPAA*, DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/ER6M-X3KL (last accessed June 4, 2024). As a provider of dental insurance, Delta Dental is clearly a "covered entity," subject to HIPAA.

[27] *Supra*, n. 10.

[28] Under HIPAA, a "business associate" is defined as, with respect to a covered entity, a person

61. Progress knew of these legal obligations, and represents on its website that it "provides [its clients] with a Business Associate Agreement to protect [their] data and help conform to [their] business's HIPAA compliance program."[29] Under its BAAs with Delta Dental Defendants, Progress acknowledges that it is subject to requirements under HIPAA, HITECH, and the Final Rule (Omnibus Rule) and agrees to protect member Personal Health Information (PHI) as required under said laws.[30]

62. As previously alleged, DDPA also entered into BAAs with each of the Delta Dental Companies of its national network which governed the transfer, use, and disclosure of Plaintiff's and Class Members' PHI.[31] DDPA is governed by HIPAA's regulations of business associates.

63. As business associates, DDPA and Progress are also required to follow regulations for safeguarding electronic medical information pursuant to the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"). *See* HITECH Act, Sec. 13400, *et seq*.; 42 U.S. Code § 17931; 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

64. Both HIPAA and HITECH obligate Progress and DDPA to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. These standards and rules require of business

---

who: "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA], including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management and repricing. . . . ." 45 C.F.R. § 160.103(1). *Business Associate*. A business associate includes an entity "that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." 45 C.F.R. § 160.103(3). As a software that transfer HIPAA protected data contracted with a HIPAA covered entity, Progress is clearly a "business associate," subject to HIPAA, with respect to its relationship and data acquired and stored through its contract with Delta Dental Defendants.

[29] *Supra*, n. 14.

[30] *See* "Business Associate Contracts," DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/7828-L5RG (last accessed June 4, 2024); *see id*. for a Sample Business Associate Agreement.

[31] *Supra*, n. 12.

associates comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained and protected. 42 U.S. Code § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities).; *see* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 45 C.F.R. § 164.316 (policies and procedures and documentation requirements).

65. As "business associates" under HIPAA, "the standards, requirements, and implementation specifications adopted under [HIPAA] apply" to both Progress and DDPA. 45 C.F.R. § 160.102(b). For example, "[a] written contract between a covered entity and business associate must . . . [among numerous other requirements] require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information . . . ." [32] *See* the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information"). Business Associates are also required to comply with the HITECH Act.[33] In other words, DDPA and Progress's non-delegable duties also arise under HIPAA and the HITECH Act.

66. Further, the U.S. Department of Health and Human Services recommends the following data security measures that business associates such as Nuance and Progress should implement to protect against some of the more common, and often successful, cyber-attack techniques. According to those guidelines, business associates should:

[32] *Supra,* n. 30; *see also supra,* n. 26. (defining Delta Dental Defendants as covered entities).
[33] *See* 42 U.S.C. § 17921(2) (incorporating "business associate" as defined in 45 C.F.R. § 160.103).

A. implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity threats and how to respond;

B. implement technologies that examine and verify that received emails do not originate from known malicious sites, scan web links or attachments included in emails for potential threats, and impede or deny the introduction of malware that may attempt to access PHI;

C. mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

D. implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

E. implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[34]

67. As "covered entities" under HIPAA, respectively, Delta Dental Defendants are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA

[34] OCR Quarter 1 2022 Cybersecurity Newsletter, U.S. DEP'T HEALTH HUM.SERVS., (Mar. 17, 2022), https://perma.cc/5L25-V4Z4 (last accessed June 4, 2024).

Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information"), as well as the Health Information Technology Economic and Clinical Health Act ("HITECH as alleged in Plaintiffs' Omnibus Set of Additional Pleading Facts and incorporated as if fully set forth herein. *See* ECF No. 908 (section V(C)(II)).[35]

68. As "covered entities" under HIPAA, Delta Dental Defendants were additionally legally obligated to comply with the Breach Notification Rule, 45 C.F.R. Part 164, Subpart D ("Notification in the Case of Breach of Unsecured Protected Health Information"), which required them to provide notice of the breach to affected individuals "without unreasonable delay and in no case later than 60 days following discovery of the breach."[36] Additionally, covered entities are required to "mitigate . . . any harmful effect . . . . of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate." 45 C.F.R. § 164.530(f).

69. As previously alleged and incorporated, Progress's customers, including Delta Dental Defendants, were required to comply with the FTC guidelines. *Inter alia*, the FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[37] *See* ECF. No. 908 (section V(C)(I)).

70. Similarly, Progress's business conduct is also governed by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or

---

[35] *See also* "Summary of the HIPAA Security Rule," DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/J2XB-5TLA (last accessed June 4, 2024).

[36] § 164.404 Notification to individuals. *Breach Notification Rule*, https://perma.cc/KM4C-F3FR (last accessed June 4, 2024). "With respect to a breach at or by a business associate, . . . the covered entity is ultimately responsible for ensuring individuals are notified[.]" *Id*.

[37] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://perma.cc/W829-XP9N (last visited June 4, 2024).

affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect sensitive consumer data, including Private Information. Various FTC publications and orders promulgated pursuant to the FTC Act also form the basis of Progress's duty. *See* ECF. No. 908 (section V(C)(I) applicable to Progress as well). Progress also knew or should have been aware of guidelines and publications by the FTC and other resources regarding cybersecurity risks and best practices.

Defendants Failed to Protect and Satisfy Their Legal Obligations

71. Despite Delta Dental Defendants' and DDPA's duty to safeguard Plaintiff's and Class Members' Private Information, Delta Dental Defendants and DDPA nevertheless employed inadequate data security measures to protect and secure the data with which they were entrusted, resulting in the Data Breach and the subsequent compromise and theft of Plaintiff's and Class Members' Private Information. As described in Plaintiffs' Omnibus Set of Additional Pleading Facts, had Delta Dental Defendants and DDPA taken their obligations seriously, they would have determined that the MOVEit software was not safe and would put Plaintiff's and Class Members' Private Information at risk. See ECF No. 908 (section V(D)).

72. Similarly, Progress failed to identify and remediate vulnerabilities in its MOVEit software and secure Plaintiff's and Class Members' Private Information despite its duties to do so, although it knew or should have known of the vulnerabilities in its software and that it was obligated to patch them. *See* ECF No. 908 (section IV).

73. Although Delta Dental Defendants owed a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their Private Information, Delta Dental Defendants maintained, stored, disclosed, shared, and/or transferred their Private Information in a negligent and/or reckless manner. In particular, their Private Information was maintained on computer systems in a condition vulnerable to cyberattacks.

74. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Delta Dental Defendants, and thus they were on notice that failing to take steps necessary to ensure their vendors, including Defendant Progress, properly safeguarded Plaintiff's and Class Members' Private Information from those risks that left their Private Information in a vulnerable condition.

75. As alleged in this Complaint, as well as more generally in the Plaintiffs' Omnibus Set of Additional Pleading Facts, ECF No. 908 (section V(C)(II)), Delta Dental Defendants failed to comply with HIPAA and HITECH, including in the following ways:

A. Failing to maintain adequate security practices, systems, and protocols to prevent data loss and theft;

B. Failing to mitigate risks of data breach and implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

C. Failing to ensure the confidentiality, integrity, and protection of electronic PHI that Delta Dental Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1).

D. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

E. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

F. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

G. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

H. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

I. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce in violation of 45 CFR 164.306(a)(94);

J. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*;

K. Retaining information past a recognized purpose and not deleting it; and

L. Failing to ensure that their third-party vendor, Progress, had implemented adequately safe and secure policies and practices.

76. Delta Dental Defendants failed to comply with FTC guidelines and industry standards as well. *See* ECF No. 908 (sections V(C)).

77. Similarly, DDPA and Progress failed to comply with HIPAA and HITECH, including in the following ways:

A. Failing to maintain adequate security practices, systems, and protocols to prevent data loss and theft;

B. Failing to mitigate risks of data breach and implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

C. Failing to ensure the confidentiality, integrity, and protection of electronic PHI that they create, receive, maintain, and/or transmit in violation of 45 CFR 164.306(a)(1);

D. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

E. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

F. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

G. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

H. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the

privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

I. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and

J. Retaining information past a recognized purpose and not deleting it.

78. Delta Dental Companies in DDPA's network have historically been subject to numerous data breaches[38] during which unauthorized agents gained access to their or their vendors' network systems, compromising the Private Information of their customers. As described herein, Delta Dental Defendants and DDPA knew based on breaches of Delta Dental Companies' networks and the prevalence of cyberattacks across the industry that the data it collected and stored was highly valuable and vulnerable. *See* ECF No. 908 (section II(G)).

79. Similarly, as alleged, Progress knew of these same risks and should have known of the vulnerabilities in its software, and by failing to patch them, failed to uphold its obligations to protect Plaintiff and Class Members' Private Information. Moreover, Progress's failure to act as quickly as possible after the breach led to additional losses for Plaintiff and Class Members. *See* ECF. No. 908 (sections IV(D)-(E)).

80. Progress's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, as well as its failure to verify whether it had implemented such measures, also constitutes an unfair act or practice prohibited by Section 5 of

[38] *See, e.g.*, "Important Security Event Notice" (breach of Delta Dental of Washington's own network systems) (2022), notice available here: https://perma.cc/DH99-EUEF (last visited June 4, 2024); "Notice of EyeMed Vision Care LLC Data Breach" (vendor of Delta Dental affiliate) (2020), notice available here: https://perma.cc/QT25-3A9N (last visited June 4, 2024).

the FTCA, 15 U.S.C. § 45 as well as FTC and industry standards and guidelines discussed throughout this Complaint. *See* ECF No. 908 (sections V(C)).

81. Although DDPA disclosed that the MOVEit Transfer servers that were the target of the Data Breach were located within the Delta Dental of California network environment, Ex. A, ¶ 9, the details otherwise of the Data Breach remain in the exclusive control of Defendants. For example, Delta Dental Defendants and DDPA did not disclose the ways in which they failed to comply with data security regulations and industry standards that made it vulnerable to the Data Breach, by way of their third-party service provider, MOVEit, or otherwise. Moreover, although it admitted to Plaintiff that their "health insurance information" and "treatment cost information" had been compromised, Delta Dental failed to indicate, for example, whether the data included the treatment itself, *i.e.*, the medical condition, which is of utmost sensitivity – public disclosure of which could lead to humiliation or other serious harms.

82. However, upon information and belief, Defendants Delta Dental and Progress breached their duties and obligations in one or more of the following ways: (i) failing to design, test, implement, monitor, and maintain reasonable software and/or network safeguards against foreseeable threats; (ii) failing to design, implement, and maintain reasonable data retention policies; (iii) failing to adequately train staff on data security; (iv) failing to comply with industry-standard data security practices; (v) failing to warn Plaintiff and Class Members of inadequate data security practices; (vi) failing to encrypt or adequately encrypt their Private Information; and (vii) otherwise failing to secure the software and hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

83. Additionally, Delta Dental Defendants failed to comply with the Breach Notification Rule by waiting an unreasonable amount of time, far longer than the permissible 60-

day limit, to disclose the Data Breach to its customers through "individual notifications" that the Data Breach had occurred following its discovery on July 6, 2023,[39] in violation of their duties as covered entities. 45 CFR §§ 164.400-414.

Delta Dental Defendants Waited Over Five Months to Notify Plaintiff and Class Members After Discovering the Data Breach

84. As described in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) and realleged herein, Defendant Progress's MOVEit software was the target of a catastrophic and devastating successful cyberattack that affected thousands of its clients and compromised the Private Information of millions of their customers, including almost seven million customers of the Delta Dental insurance member companies within DDPA's network whose Private Information was stored or otherwise in use on the MOVEit Transfer servers located within the Delta Dental of California network environment. Ex. A., ¶ 9.

85. The victims of the Data Breach were subject to the highly offensive disclosure of their sensitive, personal medical information and personal identifying information ("Private Information"). Specifically, the Private information included "names with some combination of the following: addresses, Social Security numbers, driver's license numbers or other state identification numbers, passport numbers, financial account information, tax identification numbers, individual health insurance policy numbers, and/or health information."[40]

86. The "Notice of Data Security Incident" (hereafter "Notice Letters") was sent and signed by "Delta Dental of California and Affiliates" with the address listed as 560 Mission Street, Suite 1300, San Francisco, CA 94105. The Notice Letter refers to "Delta Dental of California and affiliates" as "Company," which it defines as follows therein:

---

[39] *Supra*, n. 16; s*upra*, n. 36 ("These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach").
[40] *See supra*, n. 16.

> "The Delta Dental of California enterprise includes its affiliates Delta Dental Insurance Company; Delta Dental of the District of Columbia, Delta Dental of Delaware, Inc., Delta Dental of Pennsylvania, Delta Dental of New York, Inc., Delta Dental of West Virginia, and their affiliated companies, as well as the national DeltaCare USA network."

87. "Delta Dental of California and affiliates" sent the exact same letter to Plaintiff and Class Members who, upon information and belief, are and were at all relevant times, residents of states in which *other* Delta Dental Companies operate, *e.g.*, residents of Tennessee received a Notice Letter from "Delta Dental of California and affiliates," not from the Delta Dental Company that operates in their state through which they purchased insurance. In other words, Plaintiff and Class Members' whose dental insurance program was offered and administered by DDPA member companies other than those in California, New York, Pennsylvania, D.C., West Virginia, or Alabama, Florida, Georgia, Louisiana, Mississippi, Montana, Nevada, Utah, Texas (where DDIC offers and administers Delta Dental PPO and other dental programs), still received the Notice Letter from "Delta Dental of California and its affiliates."

88. Delta Dental Defendants waited over five months after discovering the breach to begin to send its customers Notice Letters that their data had been compromised. In the Notice Letter, Delta Dental of California and affiliates (hereafter referred to as "Company" for the purposes of describing the notification) admit to Plaintiff's and Class Members' that they were victims of a data breach, finally revealing to them that their highly sensitive, personal data was accessed by an unauthorized third party and compromised. They disclosed as follows:[41]

A. "Delta Dental of California and affiliates ('Company') experienced a data security incident involving the MOVEit Transfer ('MOVEit') software, an application used by our company and many organizations worldwide."

[41] *See supra*, n. 16.

B. "On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application."

C. "On July 6, 2023 our investigation confirmed that Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated."

89. The Company admitted to each recipient that "[on] November 27, 2023, [it] determined [their] personal information was affected."

90. Upon information and belief, the Company sent its first batch of notifications to its customers who were victims of the Data Breach that their data had been compromised December 14, 2024 – the date of the Notice of Security Incident sent to the Maine Office of Attorney's General.[42]

91. In other words, the Company waited, at minimum, six and a half months after learning about the unauthorized activity on the MOVEit Platform (June 1, 2023) before it even began to reveal this crucial information to its customers and suggested that they start taking precautions to protect their identities, *e.g.*, merely review their credit reports, or to offer them identity monitoring services due to the risks they now face as a result of the Data Breach.

92. Even after concluding its own investigation and confirming that its customers' personal identifying and personal health information had been compromised on July 6, 2024, the

[42] *Id.*

Company still waited at minimum, nearly five and a half months before it started notifying its customers directly of the breach and potential risks they faced as a result.[43]

93. However, upon information and belief, thousands of recipients received a Notice Letter from the Company dated after January 23, 2024, and up to as late as February 9, 2024— in other words, approximately eight months after the Company learned about the breach, and almost two and a half months after identifying that the Plaintiff's own Private Information was compromised on November 27, 2023.

94. When the Company finally sent notice to its customers about the Data Breach, it deliberately underplayed the Data Breach's severity and obscured the nature of the Data Breach. For example, the Notice Letter fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Data Breach was perpetrated by, and the extent to which those data elements were compromised. The Company claims that after learning about the breach on June 1, 2023 it "enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity[]" but does not specify how its steps actually mitigate the harms caused by the Data Breach or describe how these measures will prevent further breaches nor its ability to protect Plaintiff's and Class Members' Private Information from future unauthorized disclosure, as required by HIPAA, 45 CFR § 164.404.

95. In the Notice Letter, the Company also claims that "[d]ata security is a priority []. We apply security patches for known vulnerabilities provided by third-party software vendors, regularly update our capabilities to monitor potential security threats and consistently manage access to our systems and data."[44] Notably, this statement appears after informing the recipient

[43] *Supra*, n. 15.
[44] *See* Delta Dental, *Notice of Data Breach*, https://perma.cc/ESW4-SFHX (last visited June 4,

what of their data was compromised, in the "What Are We Doing" section, along with its offer of free 24 months of identity monitoring services. Thus, it is ambiguous as to whether these are new measures in place, *i.e.*, what the Company is now doing as a result of the breach, or whether these were security measures already in place. The Company does not offer any assurances or indication that these measures are reasonable or adequate to safeguard and protect Plaintiff's and Class Members' Private Information in the future or whether Plaintiff and Class Members remain vulnerable to new attacks.

96. The Company's offer of 24 months of identity monitoring services is woefully inadequate given the lifetime – not merely two years – of risks Plaintiff and Class Members each face as a result of the Data Breach.

97. The Company's offer itself indicates that it recognizes that Plaintiff and Class Members are at a present and continuing risk of identity theft and fraud as a result of the Data Breach, and that these risks arose once the Company confirmed the breach, back in July 2023—when the Company first confirmed that the Company's data had been impacted. Yet the Company has offered no measures to protect Plaintiff and Class Members from these lifetime risks they now face, and upon information and belief, have failed to offer relief for the damages they suffered due to its own negligence that left Plaintiff's and Class Members' Private Information vulnerable to attack and theft.

98. The Company merely "encourage[d] individuals to remain vigilant by reviewing bank accounts, credit reports and other financial statements closely and immediately reporting any suspicious activity to the company that maintains the account for the individual."[45] In the Notice Letter, it suggested Plaintiff and Class Members run credit reports, place a security freeze on their

2024).

[45] *Supra*, n. 16.

accounts, set up fraud alerts, and report any suspicious activity. In other words, the Company shifted the burden on to Plaintiff and Class Members to remediate their own harms and be responsible for preventing future harms.

99. As alleged, Delta Dental Defendants' unreasonable delay in notifying their customers of the Data Breach was in violation of their obligations as "covered entities" under the HIPAA Breach Notification Rule, 45 CFR § 164.404. Moreover, by failing to notify Plaintiff and Class Members that their Private Information may have been compromised as early as July 2023—when the Company first confirmed that the Company's data had been impacted, Delta Dental Defendants prevented Plaintiff and Class Members from taking reasonable precautions to try to mitigate the harms of the Data Breach, in violation of 45 C.F.R. § 164.530(f), which required Delta Dental, as covered entities, to mitigate the harmful effects of the Data Breach. To the contrary, by waiting over five months to notify affected individuals, Delta Dental Defendants exacerbated the harmful effects and risks to Plaintiff and Class Members caused by the Data Breach.

Plaintiff and Class Members Suffered Serious Harms

100. As alleged and incorporated herein, as victims of cybercriminal data breach, Plaintiff and Class Members face immediate and significant harm. *See* ECF No. 908 (sections II(E)-(I)).

101. As alleged and incorporated herein, Plaintiff and Class Members suffered injuries in numerous ways and are at risk of future injuries for the rest of their lives. *See* ECF No. 908 (section II(I)).

102. As a direct and proximate result of Defendants' collective wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent,

immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, closely reviewing and monitoring their credit reports and accounts for unauthorized activity; investigating suspicious, unauthorized activity in their financial accounts or credit; placing "freezes" and "alerts" with credit reporting agencies; contacting their financial institutions, reversing charges, closing or modifying financial accounts; sorting through dozens of phishing and spam email, text, and phone communications. This time has been lost forever and cannot be recaptured.

103. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

A. theft and misuse of their personal and financial information;

B. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

C. the untimely and inadequate notification of the Data Breach;

D. the improper disclosure of their Private Information;

E. loss of privacy;

F. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

G. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

H. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

I. nominal damages

104. While Plaintiff's and Class Members' Private Information has been stolen, Defendants continue to hold Plaintiff's and Class Members' Private Information. Particularly because Defendants have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

105. Plaintiff and Class Members have suffered from the unauthorized disclosure of their Private Information. The disclosure of their Social Security numbers and their protected health information ("PHI") in particular is highly offensive due to the sensitivity of the private and

personal data and severely consequential, accompanied by various harmful uses of their Private Information that identity thieves capitalize on. *See* ECF No. 908 (section II(F)).

Plaintiff's Experience on Behalf of Her Children

106. Plaintiff Taneisha Robertson is, and at all times mentioned herein was, an individual citizen of the State of Georgia.

107. Plaintiff Robertson is a current customer of Delta Dental Defendants, and was a customer of Delta Dental Defendants at the time of the Data Breach. She receives Delta Dental insurance through her husband's employer.

108. Plaintiff Robertson provided substantial amounts of her and her minor children's Private Information to Delta Dental Defendants as a condition of receiving dental insurance.

109. Plaintiff Robertson had the reasonable expectation and understanding that Delta Dental Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Defendants had she known that Delta Dental Defendants would not take reasonable steps to safeguard it.

110. Plaintiff Robertson received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated January 10, 2024, concerning the Data Breach. The letter stated that cybercriminals exploited a security vulnerability within the systems of one of the Company's third-party vendors, Progress, and that unauthorized actors accessed or acquired the data that the Company stored on its platform, including that of Plaintiff.

111. The Notice Letter informed Plaintiff her data had been compromised, specifically that Plaintiff's "affected information included, date of birth, Social Security number, provider name, health insurance information, and treatment cost information."[46]

112. Since the Data Breach, she has had to put a credit freeze on her account.

113. Plaintiff has received alerts that her Private Information was found on the dark web since the Data Breach occurred.

114. As a consequence of the fraudulent activity subsequent to the Breach, Plaintiff incurred $40 in costs to sign up for a credit report service.

115. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff received notifications that her information was listed on the dark web and that she has experienced an uptick in phishing emails since the Data Breach.

116. The disclosure of her "health insurance information" and "treatment cost information" and is highly offensive because of the intensely personal nature of one's personal health and medical related information and has caused her to experience anxiety and increased concerns for the loss of her, and her family's, privacy and highly sensitive Private Information, as well as anxiety over the impact of cybercriminals accessing and using her Private Information because it is now in unknown hands, putting them, and potentially her family, at grave risk of identity theft presently and ongoing, including fraud affecting her credit.

117. Plaintiff values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her or her children's Private Information

[46] Ex. B.

to Delta Dental Defendants had she known of their inadequate and lax data security policies and practices.

118. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in the Company's possession, which includes Delta Dental Defendants' possession, as well as Progress's possession, is protected and safeguarded from future breaches.

119. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts and credit to reduce the risk of future identity theft and fraud.

120. To date, as a result of the Data Breach, Plaintiff has spent several hours researching the details and checking her credit and financial accounts for any unauthorized and suspicious activity, a practice that Plaintiff will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

121. Had the Company not delayed in notifying her about the Data Breach, she could have taken precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

122. As a result of the Data Breach, Plaintiff anticipates spending considerable money and additional time on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She faced and continues to a face risk of fraud and identity theft presently that will last for her lifetime.

123. Plaintiff suffered lost time, annoyance, interference, inconvenience, and incurred expenses as a result of the Data Breach.

124. Had Plaintiff been informed that Delta Dental Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in

deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

125. Plaintiff relied on Delta Dental Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

126. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury in the form of damages and diminution in the value of her Private Information— a form of intangible property that she entrusted to Delta Dental Defendants. Plaintiff remains at a substantial and imminent risk of future harm.

CLASS ALLEGATIONS

127. Plaintiff brings this class action on behalf of her herself and the Nationwide Classes, defined below. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and, as appropriate, (c)(4) of the following Classes:

> **Delta Dental Nationwide Class**
>
> All persons in the United States who provided their Private Information to Delta Dental Defendants and/or DDPA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by Delta Dental Defendants and/or DDPA.
>
> **Progress Nationwide Class**
>
> All persons in the United States whose Private Information was compromised in the MOVEit Data Breach.

128. These definitions may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

129. The Delta Dental Nationwide Class asserts claims against Delta Dental Defendants for: negligence (Count I); negligence *per se* (Count II); breach of implied contract (Count III); breach of implied covenant of good faith and fair dealing (Count IV); breach of confidence (Count V); unjust enrichment, in the alternative (Count VI); invasion of privacy (public disclosure of private facts) (Count VII); bailment (Count VIII); breach of third-party beneficiary contract (Count IX); breach of fiduciary duty (Count X); and for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.* (Count XI); as well as against specifically Delta Dental of California for violations of California Unfair Competition Law (Count XII).

130. The Delta Dental Nationwide Class asserts claims against Delta Dental Plans Association ("DDPA") for: negligence (Count I); negligence *per se* (Count II); breach of implied contract (Count III); breach of implied covenant of good faith and fair dealing (Count IV); breach of confidence (Count V); unjust enrichment, in the alternative (Count VI); invasion of privacy (public disclosure of private facts) (Count VII); bailment (Count VIII); breach of fiduciary duty (Count X); for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.* (Count XI).

131. The Progress Nationwide Class asserts claims against Progress for: negligence (Count I); negligence *per se* (Count II); breach of implied contract (Count III); unjust enrichment, in the alternative (Count VI); invasion of privacy (public disclosure of private facts) (Count VII); bailment (Count VIII); for declaratory and injunctive relief under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.* (Count XI); violations of Massachusetts General Laws (Count XIV).

132. Pursuant to Fed. R. Civ. P. 23(a), (b)(3), and (c)(4), Plaintiff brings this action on behalf of herself and on behalf of subclasses for residents of Georgia, defined below, and seeks certification of state common law claims in the alternative to the nationwide claims, as well as

statutory claims under state data breach statutes and consumer protection statutes (Counts XII-XIII).

Delta Dental Georgia Subclass

All persons residing in the state of Georgia who provided Private Information to Delta Dental Defendants and/or DDPA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by Delta Dental Defendants and/or DDPA.

Progress Georgia Subclass

All persons residing in the state of Georgia whose Private Information was compromised in the MOVEit Data Breach.

133. Excluded from the foregoing classes are: (1) the judges presiding over the action; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

134. **Numerosity**: Class Members are so numerous that their individual joinder is impracticable, as the proposed Progress Nationwide Class includes at least 60 million members, and the proposed Delta Dental Nationwide Class includes at least 6,928,932 members— all of whom are geographically dispersed. Georgia Subclasses are also so numerous that their individual joinder is impracticable, each containing thousands of members.

135. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class Members they seek to represent.

136. **Adequacy**: Plaintiff's interests are aligned with the interests of the Class Members whom they seek to represent, and Plaintiff has retained counsel with significant experience

prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and her counsel intend to prosecute this action vigorously. All Class Members' interests are well-represented by Plaintiff and undersigned counsel.

137. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

138. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

A. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' Private Information from unauthorized access and disclosure;

B. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Private Information;

C. Whether Defendants breached their duties to protect Plaintiff's and Class Members' Private Information;

D. Whether Defendants violated the statutes alleged herein;

E. Whether Plaintiff and all other Class Members are entitled to damages and the measure of such damages and relief.

139. Given that Defendants engaged in a common course of conduct as to Plaintiff and all other Class Members, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

140. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein, including the Plaintiffs' Omnibus Set of Additional Pleading Facts. ECF No. 908.

141. Delta Dental Defendants require their customers to submit non-public personal identifying information (PII) and protected health information (PHI) ("Private Information") as a condition of becoming a customer and receiving dental insurance.

142. Delta Dental Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of their businesses, which affects commerce.

143. As customers of Delta Dental Defendants, Plaintiff and Class Members, or their dentalcare providers, continue to send Delta Dental Defendants new PHI as they receive care, *e.g.*, related to treatments and costs.

144. Plaintiff and Class Members entrusted Delta Dental Defendants with their Private Information with the reasonable understanding that their highly personal Private Information would be safeguarded and protected against unauthorized disclosure.

145. As part of its business operations, Delta Dental Defendants, as governed by HIPAA agreements, shared that information with Defendants DDPA and Progress, respectively.

146. Plaintiff and Class Members reasonably believed they were entrusting DDPA with their Private Information as well, given that Plaintiff could access their Private Information related to their Delta Dental insurance through their DDPA account, on the DDPA website— branded identically to the Delta Dental Defendant respective websites. Moreover, to sign up for an account on DDPA's webpage or request information about insurance claims or coverage, Plaintiff and Class Members were required to input their Private Information.

147. Defendants had full knowledge of the high monetary value and sensitivity of their Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

148. By assuming the responsibility to collect and store this data, as well as sharing it and utilizing it to derive business value and commercial profits, Delta Dental Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information and keep it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

149. These duties extended to Defendant DDPA, which holds itself out to the public, including to Plaintiff and Class Members, through its website, as being responsible for "employ[ing] reasonable safeguards designed to promote the security of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure" across

its 39 dental insurance membership companies, which include the Delta Dental Defendants. DDPA also utilizes their Private Information for commercial profits.

150. Delta Dental Defendants and DDPA owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected their Private Information.

151. Delta Dental Defendants' and DDPA's duty to use reasonable care arose from several sources, including but not limited to those described below.

152. Delta Dental holds itself out as a trusted provider of dental insurance. Delta Dental Defendants' and DDPA's duty to use reasonable security measures arose as a result of the special relationship that existed between Delta Dental Defendants, on the one hand, and Plaintiff and Class Members, on the other hand. That special relationship arose because Delta Dental Defendants were entrusted with their confidential Private Information, a necessary part of receiving dental insurance arose from its position as a dental insurance provider. Thus, Delta Dental Defendants were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

153. Delta Dental Defendants and DDPA owed a duty to Plaintiff and Class Members to select a software file transfer service that employed reasonable data security measures to protect their customers' Private Information.

154. The risk that unauthorized persons would attempt to gain access to Plaintiff's and Class Members' Private Information and misuse it was foreseeable to all Defendants. They had a common law duty to prevent foreseeable harm to others because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of

Defendants. By collecting, receiving, storing, and using Private Information that is routinely targeted by criminals for unauthorized access, they were obligated to act with reasonable care to protect against these foreseeable threats.

155. Given that Progress collects, stores, and uses vast amounts of Private Information and the high market value of this data, it was inevitable that unauthorized cybercriminals would at some point try to access Progress's computer networks. Defendants knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to them.

156. Delta Dental Defendants' and DDPA's Privacy Policies acknowledge their duties to adequately protect the personal and medical information of Plaintiff and Class Members in accordance with the law. Progress's Privacy Policies, as their business pertains to protected health information acknowledge their legal obligations under HIPAA as well as their duty to protect and prevent from disclosure all other data they collect and store.

157. Delta Dental Defendants had a duty to promptly and adequately notify Plaintiff and Class Members about the Data Breach, but failed to do so, and breached this duty.

158. Delta Dental Defendants had and continue to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within Delta Dental Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and continues to be necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

159. Defendants breached their duties owed to Plaintiff and Class Members and thus were negligent. Defendant breached these duties by, among other things: (a) mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security,

confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to detect the breach at the time it began or within a reasonable time thereafter; and (f) failing to follow its own policies and practices published to its clients.

160. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach and harms suffered.

161. Defendants' respective negligent conduct is ongoing, in that Plaintiff's and Class Members' Private Information remains in Defendants' possession in an unsafe and insecure manner.

162. Plaintiff and Class Members are entitled to injunctive relief requiring Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

163. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

164. Defendants had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiff's and Class Members' Private Information.

165. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect sensitive consumer data, including Private Information.

166. Various FTC publications and orders promulgated pursuant to the FTC Act also form the basis of Defendants' duty.

167. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus were negligent, by failing to implement fair, reasonable, or appropriate computer systems and data security practices that complied with applicable industry standards to safeguard Plaintiff's and Class Members' Private Information as part of its business practices.

168. Delta Dental Defendants are "covered entities" under HIPAA, and Defendants DDPA and Progress, respectively, are "business associates."

169. Delta Dental Defendants' duty to use reasonable security measures under HIPAA required Defendants to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l).

170. Delta Dental Defendants owed a duty to "reasonably safeguard protected health information from any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(2). Some or all of the healthcare and/or medical information that was compromised and stolen by the unauthorized actors constitutes "protected health information" within the meaning of HIPAA. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103.

171. As business associates, DDPA and Progress also owed these legal obligations to implement administrative, technical, and physical safeguards. 42 U.S. Code § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.[47]

172. By waiting over five months to notify affected individuals, Delta Dental Defendants exacerbated the harmful effects and risks to Plaintiff and Class Members caused by the Data Breach, in violation of 45 C.F.R. § 164.530(f).

173. Defendants' specific negligent acts and omissions, resulting in failure to comply with HIPAA and HITECH regulations include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove former employees' Private Information they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

174. Defendants' violations of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) independently constitute negligence *per se*.

[47] "The HITECH Act Summary;" https://perma.cc/HSQ6-4942 (last accessed June 4, 2024).

175. Plaintiff and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

176. The harms that have occurred are the types of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

177. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Plaintiff and Class Members.

178. In addition, under various state data security and consumer protection statutes such as those outlined herein, Defendants had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

179. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored, the high frequency of cyber-attacks that target the exact type of Private Information targeted here, and the foreseeable consequences of a data breach of that nature.

180. Plaintiff and Class Members were foreseeable victims of Defendants' violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. Defendants knew or should have known that their failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and Class Members.

181. Plaintiff and Class Members were foreseeable victims of Defendants' negligent acts and omissions. Defendants knew or should have known that their failure to implement reasonable

data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and Class Members.

182. Defendants violated their own policies by failing to maintain the confidentiality of Plaintiff's and Class Members' records; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI, and ultimately disclosing Plaintiff's and Class Members' PHI.

183. Defendant Progress violated its Business Associate Agreements ("BAA") with each of the Delta Dental Defendants under which it agreed to protect customers', including Plaintiff's and Class Members', PHI and were subject to privacy and security safeguard requirements and standards established by HIPAA, HITECH, and the Omnibus Rule.

184. Defendant DDPA violated its BAAs with each of the Delta Dental Defendants under which it agreed to protect customers', including Plaintiff's and Class Members', PHI and were subject to privacy and security safeguard requirements and standards established by HIPAA, HITECH, and the Omnibus Rule.

185. But for Defendants' violations of the applicable laws and regulations, Plaintiff's and Class Members' Private Information would not have been accessed by unauthorized parties.

186. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer injuries, including, but not limited to: (i) theft of their Private Information; (ii) costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts; (iii) costs associated with purchasing credit monitoring and identity theft protection services; (iv) lowered credit scores resulting from credit inquiries following fraudulent activities; (v) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the

actual and future consequences of the Defendant Progress's Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts; (vi) the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals; (vii) damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendants with the mutual understanding that they would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; (viii) continued and certainly increased risk of exposure to hackers and thieves of their Private Information, and additional unauthorized viewing of their Private Information that was already hacked in the Data Breach; (ix) loss of their privacy and confidentiality in their Private Information; (x) the erosion of the essential and confidential relationship with their dental insurance providers, Delta Dental Defendants, which used Progress's software and exposed them to these privacy risks; (xi) loss of personal time and opportunity costs to monitor and/or remedy harms caused by theft of their Private Information; (xii); an increase in spam calls, texts, and/or emails; and (xiii) the continued and certainly increased risk to their Private Information.

187. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

188. Finally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized

disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

189. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

190. Delta Dental Defendants and DDPA solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of their regular business practices in exchange for dental insurance.

191. Plaintiff and Class Members were required to, and did, provide their Private Information to Delta Dental Defendants in exchange for the provision of dental insurance. As alleged herein, Plaintiff also provided their Private Information to DDPA.

192. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Delta Dental Defendants on the other, is demonstrated by their conduct and course of dealing. Delta Dental Defendants required Plaintiff and Class Members to provide their Private Information as a condition of dental insurance services. Plaintiff and Class Members accepted the offers for services and complied.

193. All Defendants accepted Plaintiff's and Class Members' Private Information, whether directly from them, or through their contracts with Delta Dental Defendants.

194. Defendants relied on for their businesses, and conferred direct and indirect monetary benefit from, the Private Information provided by Plaintiff and Class Members and thus

from Plaintiff and Class Members themselves, and had full knowledge of the benefits they conferred.

195. In providing their Private Information to Delta Dental Defendants and paying Delta Dental Defendants for dental insurance and all Defendants accepting that Private Information, directly or indirectly, Plaintiff and Class Members conferred a direct benefit on them, and an indirect benefit on Progress, and entered into implied contracts with Delta Dental Defendants by which they agreed to keep such information secure and confidential, ensure protection of their Private Information from unauthorized access or disclosure, and to timely and adequately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

196. Upon accepting Plaintiff's and Class Members' Private Information, Delta Dental Defendants provided Plaintiff's and Class Members' Private Information to Progress in the course of using Progress's MOVEit software and to DDPA in their ordinary course of business as member companies of DDPA's dental insurance network.

197. Privacy Policies and Practices of Delta Dental Defendants and DDPA assure Plaintiff and Class Members of their shared practices to safeguard their Private Information and of their legal obligations to do so.

198. Plaintiff and Class Members entered these same implied contracts with Defendant DDPA, whose web platform targets new or existing customers, such as Plaintiff and Class Members. DDPA holds itself out as part of the same brand of dental insurance providers, and invites them to learn more about and sign up for dental insurance through one of its 39 Delta Dental Companies, which include Delta Dental Defendants, or to create an account, input Private Information, and request information about their personal insurance claims. Based on Plaintiff's and Class Members' interactions alone with DDPA, and/or their special and business relationship

with Delta Dental Defendants, Plaintiff and Class Members could reasonably (and correctly) believe that the Delta Dental Company from which they purchased dental insurance exchanged data with DDPA, and they could also reasonably believe that DDPA and their Delta Dental insurance provider was one and the same. For these reasons, Plaintiff and Class Members would have reasonable expectations of DDPA around privacy and security of their Private Information, just as they had of Delta Dental Defendants.

199. Defendants accepted and maintained the Private Information of Plaintiff and Class Members that they acquired either from Delta Dental Defendants or direct receipt from Plaintiff and Class Members, and thus monetarily benefitted from Plaintiff and Class Members providing their Private Information, and thus Plaintiff and Class Members entered into implied contracts with Delta Dental Defendants' business associates, revenue service providers, and file transfer software providers, including Defendants DDPA and Progress.

200. Alternatively, Plaintiff and Class Members were the intended beneficiaries of Business Associate Agreements entered into between Delta Dental Defendants and their business associates, DDPA and Progress, which governed Progress's use, disclosure, and transfer terms.

201. In entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Delta Dental Defendants' and DDPA's, and their business associates', including Progress's, data security practices complied with relevant laws and regulations and were consistent with industry standards, and that they would thoroughly vet and select vendors that adequately protect Private Information.

202. Plaintiff and Class Members would not have entrusted their Private Information to Delta Dental Defendants or DDPA in the absence of implied contracts between them that they

would keep, and require the third-party vendors they select to store, transfer, and use their Private Information in fair, secure, reasonable, and legally compliant ways.

203. Implicit in these agreement between Plaintiff and Class Members and Defendants were Defendants' obligations to: (a) take reasonable steps to safeguard that Private Information, including through proper vetting of third party vendors to whom Private Information is provided; (b) prevent unauthorized disclosure of their Private Information; (c) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (d) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain Private Information only under conditions that kept such information secure and confidential.

204. Defendants breached the implied contracts made with Plaintiff and Class Members by failing to safeguard and protect their Private Information, including by entrusting their Private Information to a vendor that fails to safeguard Private Information, by failing to delete the Private Information of Plaintiff and Class Members or requiring vendors to delete information once the relationship ended, and in the case of Delta Dental Defendants, failing to provide accurate notice to them that their Private Information was compromised as a result of the Data Breach so that they could take prompt and adequate precautions to mitigate the risks caused by the Data Breach.

205. Moreover, implied in these exchanges was a promise by Delta Dental Defendants and DDPA to ensure that the Private Information of Plaintiff and Class Members was only used in connection with the agreed-upon healthcare services.

206. Plaintiff and Class Members therefore did not receive the benefit of the bargain because they provided their Private Information in exchange for an implied agreement by Delta Dental Defendants to keep it safe and secure within its computer systems and network

environment; in addition to Delta Dental Defendants' and DDPA's implied agreement to keep it safe and secure in connection with sharing Plaintiff's and Class Members' Private Information under their BAAs and providing it to third-party vendors under distinct BAAs.

207. Similarly, Progress also breached its implied contracts with Plaintiff and Class Members by failing to keep their data secure, meanwhile conferring an indirect benefit from Plaintiff's and Class Members' Private Information.

208. Defendants' conduct and lax security unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

209. Had Delta Dental Defendants or DDPA disclosed to Plaintiff and Class Members that they did not have security practices to secure sensitive data, including adequate policies to verify the security of their third-party vendors or business associates, Plaintiff and Class Members would not have provided their Private Information to Delta Dental Defendants, and thus would not have entered into implied contracts with Delta Dental Defendants, DDPA, or Progress.

210. As a direct and proximate result of Defendants' breaches, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain and overpaying for dental insurance.

211. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

212. Plaintiff and Class Members are also entitled to injunctive relief requiring Delta Dental Defendants to, *e.g.*, (i) strengthen their data monitoring procedures; (ii) evaluate, audit, and improve their processes for vetting third party vendors and the selection processes for vendors to which Delta Dental Defendants provide sensitive Private Information; (iii) submit to future annual

audits of those systems and monitoring procedures; and (iv) immediately provide or continue providing adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA)

213. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

214. As alleged, Plaintiff and Class Members entered into implied contracts with Delta Dental Defendants and DDPA when they provided and entrusted them with their Private Information in exchange for the provision of dental insurance. In doing so, Plaintiff and Class Members entered into implied contracts with Delta Dental Defendants and DDPA by which they agreed to safeguard and protect such information to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

215. Privacy Policies and Practices of Delta Dental Defendants and DDPA assure Plaintiff and Class Members of their shared practices to safeguard their Private Information and of their legal obligations to do so under HIPAA. Defendant Progress's Privacy Policies also discuss Progress's legal obligations to protect Plaintiff and Class Members personal data, including specific legal obligations with respect to HIPAA.

216. While Delta Dental Defendants and DDPA had discretion in the specifics of how they met applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing that is inherent in every contract.

217. Delta Dental Defendants and DDPA breached this implied covenant of good faith and fair dealing when they engaged in acts and/or omissions that are declared unfair trade practices

by the FTC, HIPAA, HITECH, and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' Private Information; selection of and providing Private Information to a vendor that does not adequately safeguard Private Information; and failing to disclose to Plaintiff and Class Members at the time they provided their Private Information to Delta Dental Defendants and DDPA that their security systems and those of their vendors, *e.g.*, Defendant Progress, failed to meet applicable legal and industry standards.

218. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do. Likewise, all conditions required for Delta Dental Defendants' and DDPA's performance were met.

219. Delta Dental Defendants' and DPPA's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

220. As a direct and proximate result of Delta Dental Defendants' and DDPA's above-alleged breach of implied contract, Plaintiff and Class Members have suffered and/or will suffer harms including but not limited to: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) their

lost work time; (j) the lost value of their Private Information; (k) the lost value of access to their Private Information permitted by Delta Dental Defendants and DDPA; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (m) the lost benefit of their bargains (price premium damages in the form of overpayment for dental insurance); and (n) nominal and general damages; and other economic and non-economic harm.

221. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA)

222. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

223. Plaintiff's and Class Members' Private Information constitutes confidential and unique information. Indeed, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which enables a threat actor or cybercriminal to exploit that information during the interim. Private medical information, once disclosed and in the hands of identity thieves, can cause irreparable harm and humiliation, and can even lead to blackmail.

224. Delta Dental Defendants and DDPA were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information at all points in which they interacted with Plaintiff's and Class Members and thus made an implied promise of confidentiality to Plaintiff and Class Members by accepting their Private Information.

225. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

226. By collecting and storing Plaintiff's and Class Members' Private Information and using it for commercial gain, Delta Dental Defendants and DDPA undertook a duty of care to use reasonable means to secure and safeguard this Private Information to prevent disclosure and guard against its theft.

227. As alleged herein, Delta Dental Defendants' and DDPA's relationships with Plaintiff and Class Members were governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored, and protected in confidence—by Delta Dental Defendants, as well as by DDPA and their vendors to which Delta Dental Defendants provide that Private Information—and would not be disclosed to unauthorized third parties.

228. Plaintiff and Class Members provided their respective Private Information to Delta Dental Defendants, which are all companies within the DDPA national network. DDPA entered into Business Associate Agreements with each of the Delta Dental Defendants which govern the transfer and disclosure of protected health information between the parties, including requiring DDPA to abide by the HIPAA Security Rule.

229. Plaintiff and Class Members may sign up for an account directly with DDPA, upon which they are required to provide their Private Information, and use DDPA's platform to, for example, request information about their insurance claims, which requires them to provide DDPA with additional personal and medical related information. DDPA then works with Plaintiff's and

Class Members' individual Delta Dental Company, their respective Delta Dental Defendants, to respond.

230. Plaintiff and Class Members provided DDPA and Delta Dental Defendants their Private Information with the explicit and implicit understandings that Delta Dental Defendants and DDPA would protect and not permit their Private Information to be disseminated to any unauthorized parties.

231. Due to Delta Dental Defendants' and DDPA's failure to protect Plaintiff's and Class Members' Private Information, or retain vendors that adequately protect Private Information, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

232. As a direct and proximate cause of Delta Dental Defendants' and DDPA's actions and/or omissions, Plaintiff and Class Members have suffered damages as alleged herein.

233. But for the disclosure of Plaintiff's and Class Members' Private Information, in violation of the parties' mutual understanding of confidence, including that Delta Dental Defendants and DDPA would only provide Private Information to trusted vendors that adequately safeguard the information, Plaintiff's and Class Members' Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

234. The disclosure of Plaintiff's and Class Members' Private Information, and provision of Private Information to a vendor that does not adequately secure Private Information, constitute violations of Plaintiff's and Class Members' implicit agreement and understanding that

Delta Dental Defendants and DDPA would safeguard and protect the confidential and unique Private Information.

235. The concrete injury and harm that Plaintiff and Class Members suffered was the reasonably foreseeable result of Delta Dental Defendants' and DDPA's failure to ensure protection of their Private Information.

236. As a direct and proximate result of Delta Dental Defendants' and DDPA's conduct, Plaintiff and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in both Delta Dental Defendants' and DDPA's possession and is subject to further unauthorized disclosures; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of their Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (h) nominal damages.

237. Plaintiff and Class Members seek actual and nominal damages for these harms.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

238. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

239. Plaintiff brings this Count in the alternative to their breach of implied contract claim against Defendants (Count III).

240. Plaintiff and Class Members conferred a monetary benefit on Delta Dental Defendants in connection with obtaining dental insurance, specifically, providing them with their Private Information. In exchange, Plaintiff and Class Members should have received from Delta Dental Defendants the services or benefits that were the subject of the transaction, and they should have had their Private Information protected with adequate data security.

241. Delta Dental Defendants would be unable to engage in their regular course of business without Plaintiff's and Class Members' Private Information and accepted the monetary benefits Plaintiff and Class Members provided.

242. Plaintiff and Class Members also conferred a monetary benefit on DDPA, both directly and indirectly, and indirectly to Progress, to whom Delta Dental Defendants sent Plaintiff's and Class Members' Private Information under the terms of Business Associate Agreements. Defendants DDPA and Progress would be unable to engage in their regular course of business without that Private Information and accepted the monetary benefits from the provision of Plaintiff's and Class Members' Private Information.

243. All Defendants knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained those benefits by accepting, retaining, and using the Private Information entrusted to them. Defendants profited from Plaintiff's and Class Members' retained data and used Plaintiff's and Class Members' Private Information for business purposes.

244. Acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendants to retain that benefit without payment of the value thereof. Specifically, Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite data security.

245. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

246. Because Defendants failed to implement appropriate data management and security measures, under the principles of equity and good conscience, it would be unjust if Defendants were permitted to retain the monetary benefit belonging to Plaintiff and Class Members.

247. Defendants acquired Plaintiff and Class Members' Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

248. If Plaintiff and Class Members had known that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

249. Had Plaintiff and Class Members known that Defendants did not and would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted Defendants with their Private Information.

250. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine for themselves how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information and diminution of its value; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) future costs in terms of time, effort, and money that they will need to expend to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; (viii) emotional distress, anxiety, and inconvenience; (ix)

irreparable breach of confidence in their insurance providers; (x) loss of benefit of the bargain (price premium damages in the form of overpayment for dental insurance).

251. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm. It would be inequitable for the Defendants to retain the benefits without paying fair value for them.

252. Plaintiff and Class Members are entitled to restitution and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

253. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VII
INVASION OF PRIVACY (PUBLIC DISCLOSURE OF PRIVATE FACTS)
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

254. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

255. Plaintiff and Class Members reasonably expected that the highly personal, sensitive Private Information entrusted to Defendants, directly or indirectly, would be kept private,

confidential, and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

256. Defendants unlawfully invaded the privacy rights of Plaintiff and Class Members by:

A. Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

B. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

C. Enabling the disclosure of their personal and sensitive Private Information without their informed, voluntary, affirmative, and clear consent.

257. Plaintiff's and Class Members' Private Information, such as health information and Social Security numbers, that was publicized due to the Data Breach, was highly sensitive, private, confidential, and of no general public interest, and a reasonable person would consider its publication highly offensive and egregious.

258. A reasonable person would find it highly offensive that Defendants, having collected Plaintiff's and Class Members' sensitive Private Information, directly or indirectly, in a commercial transaction, failed to protect such Private Information from unauthorized disclosure to third parties.

259. In failing to adequately protect Plaintiff's and Class Members' sensitive Private Information, Defendants acted in reckless disregard of Plaintiff's and Class Members' privacy rights. Delta Dental Defendants and DDPA knew or should have known that their ineffective security measures, including the failure to verify and validate the security practices of their vendor, Defendant Progress, and the foreseeable consequences thereof, are highly offensive to a reasonable

person in Plaintiff's and Class Members' position. Defendant Progress knew or should have known of the risks of failing to implement adequate data security practices, too, and the foreseeability and offensiveness of such disclosures.

260. Defendants violated Plaintiff's and Class Members' right to privacy under the common law.

261. Defendants' unlawful invasions of privacy damaged Plaintiff and Class Members. As a direct and proximate result of Defendants' unlawful invasion of privacy and public disclosure of private facts, Plaintiff's and Class Members' reasonable expectations of privacy were frustrated and defeated. Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial out-of-pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial out-of-pocket costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

262. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach and these invasions of privacy.

263. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*: (i) strengthen their data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VIII
BAILMENT
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

264. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

265. Plaintiff and Class Members provided Private Information to Defendants, and Defendants were under a duty to that information keep private and confidential.

266. Defendants received this information from Plaintiff and Class Members either directly or through their dental/healthcare providers and their business associates or through one of the Delta Dental companies under a Business Associate Agreement.

267. Plaintiff's and Class Members' Private Information is personal property and was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

268. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks they took when they accepted their Private Information for safeguarding and assumed the risk voluntarily.

269. Once Defendants accepted Plaintiff's and Class Members' Private Information, they were in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

270. Defendants did not safeguard Plaintiff's or Class Members' Private Information when they failed to adopt and enforce adequate security safeguards to prevent the known risk of a cyberattack.

271. Defendants' failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

272. As a result of Defendants' failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT IX
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants)

273. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

274. Upon information and belief, Progress entered into contracts with Delta Dental Defendants to provide them with secure file transfer services, servers, and/or related equipment and services that included access to and use of the MOVEit software, data security practices, procedures, and protocols related to the MOVEit software sufficient to safeguard the Plaintiff's and Class Members' Private Information that was entrusted to Delta Dental Defendants.

275. Upon information and belief, contracts between Progress and the Delta Dental Defendants were virtually identical and were made expressly for the benefit of Delta Dental Defendants' customers, including Plaintiff and Class Members, as it was their Private Information that Progress agreed to receive, store, utilize, transfer, and protect through its services, so that Delta Dental Defendants could provide them dental insurance services. Thus, the benefit of collection,

use, and protection of the Private Information belonging to Plaintiff and Class Members was the direct and primary objective of the contracting parties, and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

276. Delta Dental Defendants and Progress knew, or should have known, that if they were to breach these contracts, Plaintiff and Class Members would be harmed.

277. Delta Dental Defendants and Progress breached these contracts by, among other things, failing to adequately secure Plaintiff's and Class Members' Private Information, and, as a result, Plaintiff and Class Members were harmed.

278. As a direct and proximate result of Delta Dental Defendants' and Progress's breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and have already sustained incidental and consequential damages including: (i) financial out-of-pocket costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial out-of-pocket costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in Delta Dental Defendants' and Progress's control, and which is subject to further breaches, so long as Delta Dental Defendants and Progress fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

279. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT X
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA

280. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

281. In light of the special relationship between Delta Dental Defendants and DDPA and Plaintiff and Class Members, Delta Dental Defendants and DDPA became fiduciaries by undertaking a guardianship of the Private Information to act primarily for the benefits of Plaintiff and Class Members. This duty included their obligations to (1) safeguard Plaintiff's and Class Members' Private Information, (2) provide timely notice to Plaintiff and Class Members in the event of a Data Breach and unauthorized disclosure, and (3) maintain complete and accurate records of what information Delta Dental Defendants and DDPA store and where they store it.

282. Delta Dental Defendants and DDPA had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with their customers, in particular, to keep secure, protected, and confidential their Private Information.

283. In order to provide Plaintiff and Class Members with dental insurance services, Delta Dental Defendants required that they provide their Private Information. This information was required to receive dental insurance through any of DDPA's 39 member companies, which transferred Plaintiff's and Class Members' Private Information to DDPA after it was provided.

284. Delta Dental Defendants and DDPA knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class Members' Private Information.

285. Delta Dental Defendants and DDPA breached their fiduciary duties owed to Plaintiff and Class Members by failing to properly protect Plaintiff's and Class Members' Private Information by ensuring the integrity of the systems where they collected, stored, and transmitted

the data. Delta Dental Defendants and DDPA further breached their fiduciary duties owed to Plaintiff and Class Members by failing to detect the Data Breach and notify and/or warn Plaintiff and Class Members of the Data Breach in a timely manner.

286. As a direct and proximate result of Delta Dental Defendants' and DDPA's breach of their fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, publication, release, theft, use, and/or viewing of their Private Information, and corresponding loss of value in their Private Information, and loss of value in their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with their effort expended and their loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Delta Dental Defendants' and DDPA's possession and is subject to further unauthorized disclosures so long as they fail to undertake appropriate and adequate measures to protect it, including to ensure that it retains vendors who adequately protect Private Information; (vi) future costs in terms of time, effort, and money that will be expended be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; (vii) the diminished value of Delta Dental Defendants' services they received; and (viii) nominal damages.

287. As a direct and proximate result of Delta Dental Defendants' and DDPA's breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other

forms of injury and/or harm, and other economic and non-economic losses. Plaintiff and Class Members seek actual and nominal damages for these harms.

COUNT XI
DECLARATORY JUDGMENT ACT
28 U.S.C. §§ 2201, *et seq.*
(On Behalf of Plaintiff and the Progress Nationwide Class, or, in the alternative, Progress Georgia Subclass, against Progress; as well as on behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, Delta Dental Georgia Subclass, against Delta Dental Defendants and DDPA (herein, Delta Dental Defendants, DDPA, and Progress referred to collectively as "Defendants"))

288. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

289. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

290. Defendants owed a duty of care to Plaintiff and Class Members, which required them to adequately monitor and safeguard Plaintiff's and Class Members' Private Information.

291. Defendants still possesses the Private Information belonging to Plaintiff and Class Members.

292. Upon information and belief, Defendants' data security measures remain inadequate.

293. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

294. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

A. Defendants owe a legal duty to secure Plaintiff's and Class Members' Private Information under the common law, HIPAA, the FTCA, the California Medical Information Act, and other state and federal laws and regulations, as set forth herein;

B. Defendants' existing data monitoring measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

C. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' Private Information.

295. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, as described in the Prayer for Relief.

296. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of Progress's systems, or the systems of Delta Dental Defendants. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable and they will be forced to bring multiple lawsuits to rectify the same conduct.

297. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs at Progress, Plaintiff and Class Members will likely be subjected to substantial

identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

298. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of Defendants' systems and network, thus preventing future injury to Plaintiff and Class Members whose Private Information would be further compromised.

COUNT XII
CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of Plaintiff and the Delta Dental Nationwide Class, or, in the alternative, on behalf of the Delta Dental Georgia Subclass, against Delta Dental of California ("DDCA")

299. Plaintiff repeats and realleges the factual allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein.

300. The servers affected by the Data Breach were controlled and managed by DDCA and held all Plaintiff's and Class Members' Private Information.

301. Plaintiff and Class Members each satisfy the definition of a "person" as provided by Cal. Bus. & Prof. Code § 17201.

302. Cal. Bus. & Prof. Code § 17204 provides that "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition" may file suit.

303. DDCA violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

304. DDCA's "unfair" acts and practices include:

A. Failure to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' Private Information from unauthorized

disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Private Information being compromised, and subsequent harms caused to Plaintiff and Class Members.

B. Failure to identify foreseeable security risks, including in its third-party vendor, Progress, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

C. Failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are entrusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; California's Consumer Privacy Act (Cal. Civ. Code § 1798.150); HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902;

D. Failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of DDCA's inadequate security practices and policies, consumers could not have reasonably avoided the harms that DDCA caused; and

E. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82 disclosure requirements.

305. DDCA engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

306. DDCA's unlawful, unfair, and deceptive acts and practices include:

A. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Private Information being compromised, and subsequent harms caused to Plaintiff and Class Members;

B. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach, unauthorized disclosure of Plaintiff's and Class Members' Private Information, and subsequent harms;

C. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U. S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, HIPAA, 45 C.F.R. §

164; and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, Plaintiff's and Class Members' Private Information being compromised, and subsequent harms caused to Plaintiff and Class Members;

307. DDCA was entrusted, either directly or indirectly, with sensitive and valuable Private Information regarding millions of consumers, including that of Plaintiff and Class Members. DDCA accepted the critical responsibility of protecting the data but kept the inadequate state of its security controls secret from the public.

308. As a direct and proximate result of DDCA's unfair, unlawful, and/or fraudulent acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for DDCA's services; loss of the value of access to their Private Information; and the value of identity and credit protection and repair services made necessary by the Data Breach.

309. DDCA's violations were, and are, willful, unfair, and unconscionable.

310. Plaintiff and Class Members have lost money and property as a result of DDCA's conduct in violation of the UCL, as stated herein and above.

311. By unfairly, and unlawfully storing, collecting, and disclosing their Private Information, DDCA has taken money or property from Plaintiff and Class Members. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

312. DDCA was aware that the healthcare industry was a frequent target of sophisticated cyberattacks due to the high market value of Private Information and was on notice of the risks posed to consumers' Private Information that it collected, stored, used, and transferred.

313. DDCA was on notice that its security and privacy policies and practices were wholly inadequate, including that of ensuring its vendors were compliant with industry standards and regulations, because of previous data breaches against Delta Dental Companies within the DDPA national network that all implement the same data security policies and practices.

314. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from DDCA's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT XIII
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT ("GUDTPA")
Ga. Code Ann. §§ 10-1-370, *et seq*.
(On Behalf of Plaintiff and the Delta Dental Georgia Subclass ("Georgia Subclass" or "Subclass") against Delta Dental Insurance Company ("DDIC") and DDPA)

315. The Georgia Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and realleges the factual allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein.

316. DDIC, DDPA, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of Ga. Code Ann. § 10-1-371(5).

317. DDIC and DDPA engaged in deceptive trade practices in the conduct of their businesses, in violation of Ga. Code Ann. § 10-1-372(a), including:

A. Representing that goods or services have characteristics that they do not have;

B. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

C. Advertising goods or services with intent not to sell them as advertised;

D. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

318. DDIC's and DDPA's deceptive acts and practices include:

A. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

B. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

C. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

D. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

E. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; and HIPAA, 45 C.F.R. § 164;

F. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiff's and Subclass Members' Private Information; and

G. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

319. DDIC's and DDPA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security policies and practices and ability to protect the confidentiality of consumers' Private Information.

320. In the course of their business, DDIC and DDPA engaged in activities with a tendency or capacity to deceive.

321. DDIC and DDPA acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Georgia Subclass Members' rights. The various breaches of Delta Dental Companies within

DDPA's network put DDPA and the other Delta Dental Companies, including DDIC, on notice that their security and privacy protections were inadequate.

322. Had DDIC and DDPA disclosed to consumers that they were not complying with industry standards or regulations or that their data systems were not secure and, thus, were vulnerable to attack, they would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

323. Instead, DDIC and DDPA were entrusted, either directly or indirectly, with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and Georgia Subclass Members. DDIC and DDPA accepted the critical responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and Georgia Subclass Members acted reasonably in relying on DDIC's and DDPA's misrepresentations and omissions, the truth of which they could not have discovered.

324. As a direct and proximate result of DDIC's and DDPA's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Georgia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for DDIC's services; loss of the value of access to their Private Information; diminution of value of Private Information; value of identity and credit protection and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as they have yet to implement the necessary policies, practices, and measures to adequately safeguard their Private Information in compliance with laws and industry standards.

325. Plaintiff and Georgia Subclass Members seek all relief allowed by law, including injunctive relief, which is necessary to prospectively protect against future data breaches, and reasonable attorneys' fees and costs, under Ga. Code Ann. § 10-1-373.

COUNT XIV
MASSACHUSETTS GENERAL LAWS CHAPTER 93A
M.G.L. ch. 93A §§ 2 and 9
(On Behalf of Plaintiff and the Progress Nationwide Class against Progress)

326. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

327. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

328. Plaintiff alleges Progress committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

329. Progress knew or should have known of the inherent risks in experiencing a data breach if they failed to maintain adequate systems and processes for keeping Plaintiff's and Class Members' Private Information safe and secure. Only Progress was in a position to ensure that their systems were sufficient to protect against harms to Plaintiff and Class Members resulting from a data security incident such as the Data Breach; instead, they failed to implement such safeguards.

330. Progress's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. Progress's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

331. Progress acknowledges that its conduct created actual harm to Plaintiff and Class Members because Progress instructed them to monitor their accounts for fraudulent conduct and identity theft.

332. Progress knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting Private Information and the importance of adequate security because of, *inter alia*, the prevalence of data breaches.

333. Progress failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiff's and Class Members' Private Information, failed to recognize in a timely manner the Data Breach, and failed to notify Plaintiff and Class Members in a timely manner that their Private Information was accessed in the Data Breach.

334. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

335. As a direct and proximate result of Progress's unfair acts and practices, Plaintiff and Class Members have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or fraudulent use of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Progress's Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy,

and other economic and non-economic losses; (vii) the continued risks to their Private Information, which remains in Progress's possession (and/or to which Progress continues to have access) and is subject to further unauthorized disclosures so long as Progress fails to undertake appropriate and adequate measures to protect it; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed Private Information.

336. Neither Plaintiff nor the other Class Members contributed to Progress's Data Breach.

337. Plaintiff sent a demand for relief, in writing, to Progress on June 4, 2024, prior to filing this complaint. Multiple Plaintiffs in consolidated actions have sent[48]—or alleged in their complaints that they would send[49]—similar demand letters as required by M.G.L. c. 93A § 9. Plaintiff has not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiff and Class Members.

---

[48] *See, e.g., Ghalem, et al. v. Progress Software Corp., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[49] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp*., 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al*., 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al*., 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al*., 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al*., 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al*., 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al*., 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al*., 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al*., 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Corp., et al*., 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al*., 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al*., 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al*., 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al*., 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al.* , 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al*., 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp*., 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al*., 23-cv-1913 (D. Md.).

338. Based on the foregoing, Plaintiff and Class Members are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

339. Pursuant to M.G.L. ch. 231, § 6B, Plaintiff and Class Members are further entitled to pre-judgment interest as a direct and proximate result of Progress's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Plaintiff and Class Members are entitled to interest in an amount according to proof.

PRAYER FOR RELIEF

340. Plaintiff, individually and on behalf of the Classes, respectfully requests that the Court grant the following relief:

a. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

b. Find in favor of Plaintiff and the Class on all counts asserted herein;

c. Award Plaintiff and the Class Members monetary damages, including actual and statutory, compensatory damages, consequential, nominal, and punitive damages, to the maximum extent as allowed by law;

d. Award compensatory, consequential, general, and nominal damages in an amount to be proven at trial;

e. Award restitution and all other forms of equitable monetary relief;

f. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein regarding to the misuse or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to

issue prompt, complete, and accurate disclosure to Plaintiff and Class Members;

g. Award injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, and to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

ii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iii. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

iv. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class members on a cloud-based database;

v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and

audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate;

xi. requiring Defendants to routinely and continually conduct internal training and education, and, on an annual basis, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;

xvi. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

xvii. requiring Defendants to implement multi-factor authentication requirements, if not already implemented;

xviii. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices.

h. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts;

i. Award a mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons.

j. Order Defendants to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiff and Class Members;

k. Order Defendants to pay the costs in notifying Class Members about the judgment and administering the claims process.

l. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowed by law;

m. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial;

n. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable;

o. Distribute any monies recovered on behalf of members of the Class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendants from retaining benefits of their wrongful conduct;

p. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity; and

q. Award such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

341. Plaintiff and Class Members hereby demand a trial by jury on all issues so triable.

Dated: June 20, 2024

Respectfully submitted,

/s/ Kristen A. Johnson

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP

100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

Andrea Gold
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue NW, Ste.1010
Washington, DC 20006
Phone: (202) 973-0900
Fax: (202) 973-0950
agold@tzlegal.com

Emily Feder Cooper
TYCKO & ZAVAREEI LLP
1970 Broadway, Ste.1070
Oakland, CA 94612
Phone: (202) 973-0900
Fax: (202) 973-0950
ecooper@tzlegal.com

Kyle McLean (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney
Email: mbarney@sirillp.com
Tyler Bean
Email: tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Plaintiff's Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 20, 2024

/s/ Kristen Johnson
Kristen Johnson